

In the Claims

1. (Currently Amended) A method of controlling access to a network, comprising:
requesting an identity from a mobile client attempting to connect to the network;
receiving the identity;
associating location information corresponding to the client with the identity;
authenticating the identity;
comparing the location information against a policy designating locations, if any, at
which the client is permitted to connect to the network; and

deciding whether to grant or deny the client access to the network based on the
authenticity of the identity and the comparison of the location information;

wherein the location information indicates the location of a network switch to which the
client is attempting to connect, and the location information indicates the association between a
particular port of the network switch and the physical location of an edge device or a wired user
station associated with the particular port of the network switch.

~~when access is granted, permitting roaming of the mobile client within the network;~~

~~during said roaming, when signal quality from a current access point in communication
with the mobile client deteriorates sufficiently, locating another access point;~~

~~when another access point is located, associating the mobile client with the newly located
access point and allowing the client to continue to access the network upon determining, by
comparing updated location information corresponding to the mobile client against the policy,
that the mobile client is still authorized to access the network~~

2. (Original) The method of claim 1, further comprising:

passing the identity and the location information to an authentication server, wherein the
authentication server performs the steps of authenticating, comparing and deciding.

3. (Previously Presented) The method of claim 2, wherein the authentication server is a RADIUS server.
4. (Original) The method of claim 1, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared encryption key, a smart card identifier, and any combination of the foregoing information.
5. (Original) The method of claim 1, wherein the client is a user station capable of connecting to the network through an access point.
6. (Original) The method of claim 1, wherein the client is a wired device capable of connecting to the network through an Ethernet switch port.
7. (Previously Presented) The method of claim 1, comprising:

using a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing to authenticate the identity.
8. (Original) The method of claim 1, wherein the location information indicates the location of a network switch to which the client is attempting to connect.
9. (Original) The method of claim 1, wherein the location information indicates the location of an edge device for connecting the client to the network.
10. (Currently Amended) A network system, comprising:

a network;

an authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity, wherein the client communicates to the authenticator from a user station;

a data structure, accessible by an authentication server, associating identities of clients

with their authorized access locations;

the authentication server, upon receiving the identity and associated location information from the authenticator, deciding whether to grant or deny the client access to the network by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure; and

~~a network manager that allows a network administrator to create and update the data structure~~

a network manager comprising an application running on a server, wherein the application permits the network administrator to create and update a policy table in the authentication server.

11. (Original) The network system of claim 10, wherein the authenticator resides in a network switch.
12. (Original) The network system of claim 10, wherein the authenticator resides in an edge device.
13. (Original) The network system of claim 10, further comprising:

an edge device for connecting a user station to a network switch.
14. (Original) The network system of claim 13, wherein the edge device is a wireless access point.
15. (Currently Amended) The network system of claim 14, wherein the user station capable of connecting to the network through the access point.
16. (Original) The network system of claim 10, wherein the client is a wired device capable of connecting to a network switch through an Ethernet port.

17. (Original) The network system of claim 10, wherein the location information indicates the location of a network switch to which the client is attempting to connect.
18. (Original) The network system of claim 10, wherein the location information indicates the location of an edge device for connecting the client to the network.
19. (Original) The network system of claim 18, further comprising an interface for permitting an administrator to associate the location information to the edge device.
20. (Original) The network system of claim 10, wherein the authentication server is included in a network switch.
21. (Original) The network system of claim 10, wherein the authentication server authenticates the identity.
22. (Original) The network system of claim 10, wherein the authentication server includes a policy designating locations, if any, at which the client is permitted to connect to the network.
23. (Previously Presented) The network system of claim 10, wherein
the authentication server is a RADIUS server.
24. (Original) The network system of claim 10, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.
25. (Previously Presented) The network system of claim 10, further comprising a network switch that comprises:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

26. (Original) The network system of claim 10, wherein the authentication server comprises:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

27. (Currently Amended) A network system, comprising:

a plurality of edge devices capable of communicating with a plurality of user stations over one or more wireless channels;

~~a network switch including a plurality of ports for connecting the edge devices to a network;~~

one or more network switches;

~~an~~ a first application running on the one or more network switches ~~network switch~~, for requesting station identities from the user stations and for associating corresponding location information with each of the station identities;

~~a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;~~

~~the~~ an authentication server for deciding whether to grant or deny each of the user stations access to the network based upon the corresponding identify and location information ~~by accessing the data structure and determining, for each user station, that the location information corresponding to the user station specifies a location that is one of the authorized access locations, if any, for the user station as maintained in the data structure; and~~

~~a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure;~~

a network manager comprising a server that runs an application that permits a network administrator to configure the location information and software images stored in the one or more switches; and

a network that connects the network manager, the authentication server and the one or more switches;

wherein the network manager either (1) connects to the network or (2) directly connects to the one or more switches and directly connects to the authentication server,

whereby when the network manager directly connects to the one or more switches and the authentication server, the network is bypassed.

28. (Original) The system of claim 27, wherein at least one of the edge devices is a wireless access point.
29. (Currently Amended) The system of claim 27, further comprising a user station that is a wired device for directly connecting to one of the ports of the network switch.
30. (Original) The system of claim 27, wherein the location information indicates the location of the network switch.
31. (Original) The system of claim 27, wherein the location information indicates the location of one of the edge devices.
32. (Original) The system of claim 27, wherein the network switch includes an interface for permitting an administrator to associate the location information to the edge devices.
33. (Original) The system of claim 27, wherein the network switch includes an authenticator for authenticating the station identities.
34. (Original) The system of claim 27, wherein the authentication server authenticates the station identities.
35. (Original) The system of claim 27, wherein the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network.

36. (Previously Presented) The system of claim 27, wherein
the authentication server is a RADIUS serve.
37. (Original) The system of claim 27, wherein the station identities includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.
38. (Previously Presented) The system of claim 27, further comprising:
an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.
39. (Currently Amended) A network system for controlling access to a network, comprising:
means for requesting an identity from a mobile client attempting to connect to the network;
means for receiving the identity;
first associating means for associating location information corresponding to the client with the identity;
authenticating means for authenticating the identity;
means for comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network;
means for deciding whether to grant or deny the client access to the network based on the authenticity of the identity and the comparison of the location information, and, ~~when access is granted, permitting roaming of the mobile client within the network;~~
~~means for locating another access point upon detecting, during said roaming, when signal quality from a current access point in communication with the mobile client has deteriorated~~

sufficiently;

~~second associating means for associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network, and~~

a means for network management comprising a means for a server that runs an application that permits a network administrator the means to configure the location information and software images stored in means for switching; and

a network means that connects the means for network management, the means for authentication and the means for switching;

wherein the network system further comprises a means for network management, wherein the means for network management configures the means for authenticating,

wherein the means for network management either (1) connects to the network or (2) directly connects to the means for switching and directly connects to the means for authentication,

whereby when the means for network management directly connects to the means for switching and the means for authentication, the means for network is bypassed.

40. (Original) The system of claim 39, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

41. (Original) The system of claim 39, wherein the client is a wireless device capable of connecting to the network through an access point.

42. (Original) The system of claim 39, wherein the client is a wired device capable of connecting to the network through an Ethernet port.

43. (Currently Amended) The system of claim 39, wherein the ~~authenticating means~~ means for authentication includes:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

44. (Original) The system of claim 39, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

45. (Original) The system of claim 39, wherein the location information indicates the location of a edge device for connecting the client to a network switch.

46. (Currently Amended) The method of claim 1 wherein the mobile client is associated with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network.

47. (Currently Amended) The system of claim 39 wherein the second associating means associates the mobile client with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access to the network.

48. (Previously Presented) The method of claim 8, wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect.

49. (Previously Presented) The network system of claim 17, wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect.

50. (Previously Presented) The network system of claim 24, wherein the identity includes a smart card identifier.

51. (Previously Presented) The system of claim 37, wherein the station identities includes a smart card identifier.